

CUSERID

Never rely on username for security - (Function is obsolete)

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-03-22

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4441 bytes

Attack Category	<ul style="list-style-type: none">• Privilege Exploitation		
Vulnerability Category	<ul style="list-style-type: none">• Access Control		
Software Context	<ul style="list-style-type: none">• Authorization		
Location	<ul style="list-style-type: none">• stdio.h		
Description	<p>cuserid(char *s) generates a character-string representation of the user name corresponding to the effective user ID of the process. If s is a NULL pointer, this representation is generated in an internal static area, the address of which is returned. Otherwise, s is assumed to point to an array of at least L_cuserid characters; the representation is left in this array. The constant L_cuserid is defined in the <stdio.h>header file.</p> <p>Never rely on username for security.</p> <p>cuserid() should be considered obsolete. This function has been or will be deprecated in several systems (e.g., HPUnix. ISO POSIX-1). Additionally this function has changed capability within a given OS (HP).</p>		
APIs	Function Name	Comments	
	cuserid		
Method of Attack			
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Generally applicable	Convert to getpwuid (getuid()), getpwuid (geteuid()), or getlogin(), depending on	Effective.

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

		which user name is desired.	
Signature Details	char *cuserid(char *s);		
Examples of Incorrect Code	<pre>// The function is deprecated char *t_userid; #ifdef __GNUCC__ (int)t_userid = cuserid((char *) NULL); #else t_userid = cuserid((char *) NULL); #endif /*</pre>		
Examples of Corrected Code	<pre>void user_name(void) { /* See the getpwuid man page * for a description of the * structure. */ struct passwd *passwd; /* Get the uid of the running * process and use it to get * a record from /etc/passwd */ passwd=getpwuid(getuid()); printf("Users Real name is %s\n", passwd->pw_gecos); }</pre>		
Source References	<ul style="list-style-type: none"> cuserid manpage HP-UX Reference. cuserid(3S² 		
Recommended Resource			
Discriminant Set	Operating System	<ul style="list-style-type: none"> Windows 	
	Languages	<ul style="list-style-type: none"> C C++ 	

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

1. <mailto:copyright@cigital.com>

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.